

PATENT

**B. AMENDMENTS TO THE CLAIMS**

1. (currently amended) A method for securely transmitting data in a network, said method comprising:  
sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers;  
receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data;  
establishing a secure connection between a plurality of computers the first computer and the second computer; and  
transmitting a password across the secure connection, the password used to encrypt and decipher the data;  
encrypting the data using the password; and  
transmitting the encrypted data encrypted using the password over a non-secure connection.

2. (original) The method as described in claim 1 further comprising:  
automatically sending a second password based on an event, the second password replacing the password as the encryption key.

3. (original) The method as described in claim 2 wherein the event includes a time interval event.

4. (original) The method as described in claim 2 wherein the event includes a preset number of transmissions

Docket No. AUS90000264US1

Page 3  
McBrearty, et al. - 09/594,517

Atty Ref. No. IBM-0015

**PATENT**

occurring between two or more computers within the plurality of computers.

5. (original) The method as described in claim 1 wherein the network includes the Internet.

6. (cancelled)

7. (original) The method as described in claim 1 further comprising:  
changing the password by including a counter as part of the password; and  
wherein the counter is incremented after each transmission between the first and second computer systems.

8. (original) The method as described in claim 1 wherein the data is selectively encrypted.

9. (currently amended) The method as described in claim 1 wherein the selection is based on determining a sensitivity corresponding to the data.

10. (original) The method as described in claim 1 wherein the deciphering further comprises:  
analyzing the data packet and determining whether the data packet is encrypted; and  
selectively deciphering the data packet based on the analyzing.

11. (currently amended) A computer system comprising:

Docket No. AUS90000264US1

Page 4  
McBrearty, et al. - 09/594,517

Atty Ref. No. IBM-0015

PATENT

a networked computer system including a plurality of computers connected by a computer network, each of the computers including:

one or more processors;

a memory connected to the processors; and

a network connection that connects the computer with the computer network;

and

an encryption tool, the encryption tool including:

means for sending a request from the first computer system to the second computer system prior to establishing a secure connection, the first computer system and the second computer system included in a plurality of computer systems;

means for receiving a response from the second computer system, the response indicating that the second computer system accepts packets of data that is encrypted;

means for establishing a the secure connection between a the first computer system and a the second computer system, each of the computer systems connected to a computer network;

means for sending a password from the first computer system to the second computer system across the secure connection;

means for encrypting one or more packets of data using the password as an encryption key;

means for transmitting one or more of the encrypted packets of data from one of the

PATENT

computer systems to the other computer system;  
and  
means for deciphering the one or more encrypted  
packets of data at the receiving computer system  
using the password as the encryption key.

12. (original) The computer system as described in claim 11 wherein the computer network is a private network.

13. (original) The computer system as described in claim 11 wherein the encryption tool further includes:  
means for sending a second password, the second password replacing the password as the encryption key.

14. (cancelled)

15. (original) The computer system as described in claim 14 wherein the means for sending is performed on a defined time interval.

16. (original) The computer system as described in claim 14 wherein the means for sending is performed after a preset number of transmissions between the first and second computer systems.

17. (original) The computer system as described in claim 11 wherein the computer network includes the Internet.

18. (original) The computer system as described in claim 11 wherein the encryption tool further includes:

## PATENT

means for changing the password by including a counter as part of the password; wherein the counter is incremented after each transmission between the first and second computer systems.

19. (currently amended) A computer program product in a computer usable medium for encrypting data between computers, said computer program product comprising:  
means for sending a request from a first computer system to a second computer system prior to establishing a secure connection, the first computer system and the second computer system included in a plurality of computer systems;  
means for receiving a response from the second computer system, whereby the response informs the first computer system that the second computer system accepts encrypted data;  
means for establishing a the secure connection between a the first computer system and a the second computer system, each of the computer systems connected to a computer network;  
means for sending a password from the first computer system to the second computer system across the secure connection;  
means for encrypting one or more packets of data using the password as an encryption key and means for deciphering the data packets using the password as the encryption key.

PATENT

20. (original) The computer program product as described in claim 19 further comprising:  
means for transmitting the one or more packets of data from one of the computer systems to the other computer system; and  
means for deciphering the one or more packets of data at the receiving computer system using the password as the encryption key.
21. (original) The computer program product as described in claim 19 further comprising:  
means for sending a second password, the second password replacing the password as the encryption key.
22. (cancelled)
23. (original) The computer program product as described in claim 19 further comprising:  
means for changing the password by including a counter as part of the password, wherein the counter is incremented after each transmission between the first and second computer systems.
24. (original) The computer program product as described in claim 19 wherein the computer network includes a private network.
25. (original) The computer program product as described in claim 19 wherein the means for encrypting further comprises:

PATENT

means for determining whether the data packets include sensitive information; and means for selectively performing the encrypting based on the determination.

26. (original) The computer program product as described in claim 19 wherein the means for deciphering further comprises:

means for analyzing the data packet and determining whether the data packet is encrypted; and means for selectively deciphering the data packet based on the analysis.

27. (currently amended) A method for transmitting data securely between computers, said method comprising: establishing a secure connection between a first computer system and a second computer system, each of the computer systems connected to a computer network; sending a password from the first computer system to the second computer system across the secure connection; encrypting one or more packets of data using the password as an encryption key and responsive to deciphering the data packets using the password as the encryption key; transmitting the one or more packets of data from one of the computer systems to the other computer system; deciphering the one or more packets of data at the receiving computer system using the password as the encryption key;

**PATENT**

*a*  
sending a request from the first computer system to the second computer system prior to the establishing of the secure connection; and responding to the request by the second computer system, the response further including: informing the first computer system that the second computer system accepts the data that is encrypted data.

---